

INTEROPERABILIDADE E CONECTIVIDADE EM ECOSSISTEMAS IOT HETEROGÊNEOS: DESAFIOS E SOLUÇÕES PARA REDES INTELIGENTES DE GRANDE ESCALA

INTEROPERABILITY AND CONNECTIVITY IN HETEROGENEOUS IOT
ECOSYSTEMS: CHALLENGES AND SOLUTIONS FOR LARGE-SCALE
INTELLIGENT NETWORKS

Ciências Exatas e da Terra, Engenharias • 14/07/2026

REGISTRO DOI: [10.70773/revistatopicos/783482931](https://doi.org/10.70773/revistatopicos/783482931)

Rômulo Ferreira dos Santos¹

RESUMO

A consolidação da Internet das Coisas depende da capacidade de integrar dispositivos com características técnicas distintas em ambientes operacionais altamente distribuídos, dinâmicos e heterogêneos. Sensores, atuadores, gateways, plataformas em nuvem, sistemas embarcados, redes industriais, dispositivos domésticos inteligentes, aplicações urbanas, máquinas conectadas, veículos, equipamentos médicos e sistemas de automação operam frequentemente com protocolos, padrões de dados, restrições energéticas, capacidades computacionais e requisitos de segurança diferentes. Este estudo investiga os desafios relacionados à interoperabilidade, comunicação, segurança, escalabilidade e governança em redes IoT heterogêneas, propondo uma arquitetura intermediária voltada à padronização da troca de informações entre dispositivos inteligentes. A pesquisa adota abordagem qualitativa, exploratória, bibliográfica e propositiva, fundamentada em literatura sobre Internet das Coisas, sistemas distribuídos, middleware, computação em borda, protocolos leves, interoperabilidade semântica, arquiteturas orientadas a eventos, segurança cibernética e redes inteligentes de grande escala. Discute-se a relevância de padrões como MQTT, CoAP, OPC UA, oneM2M, W3C Web of Things, NGSI-LD e Matter para a construção de ecossistemas conectados mais confiáveis, interoperáveis e escaláveis. Propõe-se a Arquitetura Intermediária de Mediação para IoT Heterogênea, denominada AIM-IoT, composta por camadas de conectividade, adaptação de protocolos, mediação semântica, gerenciamento de contexto, segurança, observabilidade, orquestração de borda e governança de dados. Os resultados indicam que mecanismos flexíveis de integração favorecem maior estabilidade da rede, reduzem perdas de comunicação, aumentam a confiabilidade dos sistemas distribuídos e ampliam a capacidade de evolução dos ecossistemas

conectados. Conclui-se que a interoperabilidade em IoT não deve ser tratada apenas como compatibilidade técnica, mas como condição estrutural para segurança, escalabilidade, sustentabilidade operacional e inovação em aplicações industriais, urbanas, ambientais, agrícolas, logísticas e residenciais inteligentes.

Palavras-chave: Internet das Coisas; interoperabilidade; redes inteligentes; conectividade; sistemas distribuídos; middleware; segurança IoT; computação em borda.

ABSTRACT

The consolidation of the Internet of Things depends on the ability to integrate devices with different technical characteristics in highly distributed, dynamic, and heterogeneous operational environments. Sensors, actuators, gateways, cloud platforms, embedded systems, industrial networks, smart home devices, urban applications, connected machines, vehicles, medical equipment, and automation systems often operate with different protocols, data standards, energy constraints, computational capacities, and security requirements. This study investigates challenges related to interoperability, communication, security, scalability, and governance in heterogeneous IoT networks, proposing an intermediate architecture aimed at standardizing information exchange among intelligent devices. The research adopts a qualitative, exploratory, bibliographic, and propositional approach based on literature on the Internet of Things, distributed systems, middleware, edge computing, lightweight protocols, semantic interoperability, event-driven architectures, cybersecurity, and large-scale intelligent networks. The article discusses the relevance of standards such as MQTT, CoAP, OPC UA, oneM2M, W3C Web of Things, NGSI-LD, and Matter for building more reliable, interoperable, and scalable connected ecosystems. It proposes the Intermediate Mediation

Architecture for Heterogeneous IoT, named AIM-IoT, composed of layers of connectivity, protocol adaptation, semantic mediation, context management, security, observability, edge orchestration, and data governance. The results indicate that flexible integration mechanisms favor greater network stability, reduce communication losses, increase the reliability of distributed systems, and expand the evolutionary capacity of connected ecosystems. The article concludes that IoT interoperability should not be treated merely as technical compatibility, but as a structural condition for security, scalability, operational sustainability, and innovation in industrial, urban, environmental, agricultural, logistics, and smart residential applications.

Keywords: Internet of Things; interoperability; intelligent networks; connectivity; distributed systems; middleware; IoT security; edge computing.

1. INTRODUÇÃO

A Internet das Coisas tornou-se uma das bases tecnológicas mais relevantes da transformação digital contemporânea, permitindo a conexão entre objetos físicos, sensores, atuadores, plataformas computacionais e serviços digitais. A proposta central da IoT é transformar objetos antes isolados em elementos comunicantes, capazes de coletar dados, processar informações, interagir com outros sistemas e apoiar decisões automatizadas ou semiautomatizadas em diferentes contextos, como indústria, cidades inteligentes, saúde, agricultura, logística, energia, residências conectadas e monitoramento ambiental (ATZORI; IERA; MORABITO, 2010; GUBBI et al., 2013; AL-FUQAHA et al., 2015).

O crescimento da IoT, entretanto, não ocorre de forma homogênea. Os ecossistemas conectados são compostos por dispositivos com capacidades técnicas muito distintas. Alguns sensores possuem baixa capacidade computacional, pouca memória e alimentação por bateria; outros dispositivos industriais operam em redes cabeadas robustas; gateways realizam pré-processamento local; plataformas em nuvem armazenam grandes volumes de dados; aplicações analíticas consomem fluxos contínuos de eventos; e sistemas legados precisam coexistir com novos protocolos digitais (BORGIA, 2014; PERERA et al., 2014; SANTOS et al., 2020).

Essa diversidade cria um dos maiores desafios da IoT: a interoperabilidade. Interoperar significa permitir que sistemas, dispositivos, aplicações e organizações diferentes consigam trocar informações, compreender dados, coordenar ações e manter funcionamento integrado, mesmo quando foram desenvolvidos por fabricantes, padrões, arquiteturas e finalidades diferentes. Em IoT, a interoperabilidade não é apenas conveniência técnica; é condição para escalabilidade, segurança, confiabilidade e viabilidade econômica (ATZORI; IERA; MORABITO, 2010; GUBBI et al., 2013; W3C, 2023).

A heterogeneidade manifesta-se em diferentes níveis. No nível físico, há múltiplas tecnologias de comunicação, como Wi-Fi, Bluetooth Low Energy, Zigbee, Thread, LoRaWAN, NB-IoT, Ethernet, 5G, RFID e IEEE 802.15.4. No nível de rede e transporte, coexistem IPv6, 6LoWPAN, TCP, UDP, RPL e diferentes mecanismos de roteamento. No nível de aplicação, protocolos como MQTT, CoAP, HTTP, AMQP, OPC UA e DDS são utilizados conforme o domínio. No nível semântico, dados podem representar a mesma realidade com

nomes, unidades, formatos e ontologias diferentes (SHELBY; BORMANN, 2009; WINTER et al., 2012; AL-FUQAHA et al., 2015).

Essa fragmentação dificulta a integração de soluções. Um sensor de temperatura pode enviar dados em JSON por MQTT; outro pode utilizar CoAP; uma máquina industrial pode expor dados via OPC UA; um sistema urbano pode organizar informações em NGS-LD; uma residência inteligente pode usar Matter; e uma plataforma corporativa pode exigir APIs REST ou eventos em Kafka. Sem mediação, cada integração torna-se específica, cara, frágil e difícil de manter (KOVATSCHEK; MAYER; OSTERMAIER, 2012; OPC FOUNDATION, 2023; W3C, 2023).

A interoperabilidade também envolve segurança. Dispositivos IoT frequentemente possuem limitações de hardware, ciclos longos de vida útil, dificuldade de atualização, exposição física, credenciais fracas e integração com redes críticas. Vulnerabilidades em dispositivos aparentemente simples podem comprometer sistemas industriais, residenciais, hospitalares ou urbanos. Portanto, a conectividade sem segurança amplia superfície de ataque e risco sistêmico (ROMAN; ZHOU; LOPEZ, 2013; SICARI et al., 2015; NIST, 2020).

Em redes inteligentes de grande escala, a conectividade precisa ser estável, tolerante a falhas e adaptativa. Ambientes IoT podem envolver milhares ou milhões de dispositivos, comunicação intermitente, perda de pacotes, baixa largura de banda, latência variável, interferência, restrições energéticas e mobilidade. A arquitetura precisa suportar crescimento, falhas parciais, atualização contínua e diversidade de aplicações (BUYYA; DASTJERDI, 2016; SHI et al., 2016; SATYANARAYANAN, 2017).

Diante desse cenário, este artigo parte do seguinte problema de pesquisa: **como estruturar uma arquitetura intermediária capaz de promover interoperabilidade, conectividade, segurança e escalabilidade em ecossistemas IoT heterogêneos de grande escala?**

O objetivo geral é analisar os desafios de interoperabilidade e conectividade em ecossistemas IoT heterogêneos, propondo uma arquitetura intermediária de mediação para padronização da troca de informações entre dispositivos inteligentes. Como objetivos específicos, busca-se: discutir a natureza da heterogeneidade em IoT; examinar os principais protocolos e padrões de comunicação; analisar desafios de segurança e confiabilidade; propor camadas de mediação semântica, adaptação de protocolos e gerenciamento de contexto; e refletir sobre aplicações industriais, urbanas e residenciais inteligentes (AL-FUQAHA et al., 2015; SICARI et al., 2015; W3C, 2023).

Defende-se como tese central que a interoperabilidade em IoT deve ser tratada como arquitetura sistêmica, e não como simples compatibilidade pontual entre dispositivos. A consolidação de redes inteligentes de grande escala depende de middleware, ontologias, APIs padronizadas, gateways de borda, segurança por projeto, observabilidade e governança de dados (ATZORI; IERA; MORABITO, 2010; GUBBI et al., 2013; NIST, 2020).

2. METODOLOGIA

Este estudo adota abordagem qualitativa, exploratória, bibliográfica e propositiva. A escolha por esse delineamento justifica-se pela natureza interdisciplinar do tema, que envolve redes de

computadores, sistemas distribuídos, engenharia de software, segurança cibernética, arquitetura de sistemas, computação em borda, Internet das Coisas, inteligência distribuída e padronização tecnológica (CRESWELL, 2014; TORRACO, 2005).

A pesquisa foi estruturada como revisão narrativa integrativa com proposição de arquitetura conceitual. Esse tipo de revisão é adequado para temas tecnológicos emergentes, nos quais a literatura está distribuída em artigos acadêmicos, documentos de padronização, relatórios técnicos, especificações industriais e estudos de aplicação (WHITTEMORE; KNAFL, 2005; SANTOS et al., 2020).

A pergunta norteadora foi: **quais componentes técnicos, semânticos, comunicacionais e de segurança devem compor uma arquitetura intermediária para interoperabilidade em ecossistemas IoT heterogêneos?**

Foram considerados como eixos de análise: Internet das Coisas; heterogeneidade de dispositivos; protocolos de comunicação; middleware; interoperabilidade sintática; interoperabilidade semântica; gerenciamento de contexto; computação em borda; arquiteturas publish/subscribe; segurança IoT; escalabilidade; confiabilidade; observabilidade; governança de dados; e aplicações em redes inteligentes de grande escala (ATZORI; IERA; MORABITO, 2010; GUBBI et al., 2013; AL-FUQAHA et al., 2015).

Entre os autores e documentos utilizados, destacam-se Atzori, Iera e Morabito (2010), Gubbi et al. (2013), Al-Fuqaha et al. (2015), Borgia (2014), Perera et al. (2014), Roman, Zhou e Lopez (2013), Sicari et al. (2015), Buyya e Dastjerdi (2016), Shi et al. (2016), Satyanarayanan

(2017), Shelby, Hartke e Bormann (2014), Banks et al. (2019), Kovatsch, Mayer e Ostermaier (2012), Noura, Atiquzzaman e Gaedke (2019), W3C (2023), oneM2M (2024), ETSI (2020), NIST (2020) e OPC Foundation (2023).

Foram incluídas publicações e especificações relacionadas a IoT, interoperabilidade, protocolos de comunicação, middleware, segurança, redes heterogêneas, edge computing, sistemas distribuídos e padrões abertos. Foram excluídos textos exclusivamente promocionais, materiais sem autoria identificável, publicações sem relação direta com conectividade e interoperabilidade, além de estudos restritos a um único dispositivo sem implicações arquiteturais.

A análise foi organizada em quatro etapas. A primeira consistiu no mapeamento dos níveis de heterogeneidade em IoT: física, conectividade, protocolo, dados, semântica, segurança, aplicação e governança. A segunda etapa examinou padrões e tecnologias aplicáveis, incluindo MQTT, CoAP, OPC UA, Matter, oneM2M, W3C Web of Things e NGSI-LD. A terceira etapa identificou requisitos de uma arquitetura intermediária, como adaptação de protocolos, normalização de dados, descoberta de dispositivos, autenticação, autorização, monitoramento e gerenciamento de contexto. A quarta etapa resultou na proposição da **AIM-IoT — Arquitetura Intermediária de Mediação para IoT Heterogênea**.

Por se tratar de estudo propositivo, a arquitetura apresentada não pretende substituir padrões existentes. Sua finalidade é integrar padrões e tecnologias por meio de camadas intermediárias, facilitando a interoperabilidade entre dispositivos, plataformas e aplicações em ecossistemas de grande escala.

3. FUNDAMENTOS DA INTERNET DAS COISAS E DOS ECOSISTEMAS HETEROGÊNEOS

A Internet das Coisas pode ser compreendida como paradigma tecnológico no qual objetos físicos passam a possuir identidade digital, capacidade sensorial, conectividade e possibilidade de interação com outros dispositivos e sistemas computacionais. Essa definição amplia a internet tradicional, antes centrada em pessoas e computadores, para uma rede de coisas, ambientes, máquinas e processos conectados (ATZORI; IERA; MORABITO, 2010; GUBBI et al., 2013).

A IoT articula três dimensões fundamentais: percepção, comunicação e inteligência. A percepção envolve sensores e atuadores capazes de coletar dados ou modificar o ambiente. A comunicação permite transmitir informações por redes locais, celulares, industriais ou de longa distância. A inteligência envolve processamento, análise, automação, tomada de decisão e integração com serviços digitais (BORGIA, 2014; AL-FUQAHA et al., 2015).

Os ecossistemas IoT são heterogêneos porque não existe um único tipo de dispositivo, protocolo, dado ou aplicação. Em uma cidade inteligente, sensores ambientais podem coexistir com câmeras, semáforos, estações meteorológicas, sistemas de transporte, iluminação pública e plataformas de defesa civil. Em uma indústria, máquinas legadas podem operar ao lado de robôs, controladores lógicos programáveis, sensores sem fio, sistemas SCADA e plataformas analíticas em nuvem (ZANELLA et al., 2014; OPC FOUNDATION, 2023).

A heterogeneidade também decorre das restrições dos dispositivos. Muitos sensores são alimentados por bateria e precisam operar por anos com baixo consumo energético. Outros estão conectados à rede elétrica e podem processar mais dados. Alguns possuem memória e CPU limitadas; outros operam com sistemas embarcados robustos. Essa diversidade exige protocolos flexíveis e arquiteturas adaptativas (SHELBY; BORMANN, 2009; AL-FUQAHA et al., 2015).

A conectividade é igualmente variada. Aplicações de curta distância podem utilizar Bluetooth Low Energy, Zigbee ou Thread. Ambientes industriais podem utilizar Ethernet industrial, OPC UA ou protocolos proprietários. Aplicações de longo alcance e baixo consumo podem usar LoRaWAN ou NB-IoT. Sistemas de alta largura de banda podem utilizar Wi-Fi, 5G ou fibra óptica. Cada tecnologia possui vantagens, limitações e custos (AL-FUQAHA et al., 2015; GUBBI et al., 2013).

Além da conectividade física, há heterogeneidade de modelos de dados. Um sensor pode representar temperatura em Celsius, outro em Fahrenheit; um dispositivo pode usar “temp”, outro “temperature”; um sistema pode incluir metadados de localização, outro não; um equipamento industrial pode utilizar modelo semântico próprio. Sem padronização, os dados tornam-se difíceis de comparar, integrar e analisar (PERERA et al., 2014; W3C, 2023).

Essa diversidade é natural e inevitável. A IoT não se consolidará por meio de um único padrão universal absoluto. A solução mais realista é criar mecanismos de mediação capazes de traduzir, normalizar, contextualizar e proteger a comunicação entre sistemas heterogêneos. Essa é a função estratégica do middleware e das arquiteturas intermediárias (NOURA; ATIQUEZZAMAN; GAEDKE, 2019; KOVATSCH; MAYER; OSTERMAIER, 2012).

4. INTEROPERABILIDADE EM IOT: NÍVEIS, DIMENSÕES E DESAFIOS

A interoperabilidade em IoT pode ser analisada em quatro níveis principais: técnico, sintático, semântico e organizacional. A interoperabilidade técnica refere-se à capacidade de dispositivos se conectarem e transmitirem dados por redes compatíveis. A interoperabilidade sintática envolve formatos comuns de dados e mensagens. A interoperabilidade semântica garante que o significado dos dados seja compreendido por diferentes sistemas. A interoperabilidade organizacional envolve processos, governança, políticas e acordos entre atores (NOURA; ATIQUZZAMAN; GAEDKE, 2019; W3C, 2023).

A interoperabilidade técnica é o primeiro desafio. Dispositivos que utilizam diferentes tecnologias de comunicação podem não se comunicar diretamente. Um sensor Zigbee não fala nativamente com um servidor MQTT sem um gateway; um dispositivo industrial OPC UA pode precisar de adaptação para enviar eventos a uma plataforma de dados; um sensor CoAP pode exigir conversão para HTTP ou MQTT em ambientes de nuvem (KOVATSCH; MAYER; OSTERMAIER, 2012; OPC FOUNDATION, 2023).

A interoperabilidade sintática aparece quando sistemas conseguem transmitir dados, mas usam formatos diferentes. JSON, XML, CBOR, Protocol Buffers, SenML e formatos proprietários podem representar informações de maneira incompatível. A padronização sintática reduz erros de integração e facilita processamento automático (SHELBY; HARTKE; BORMANN, 2014; AL-FUQAHA et al., 2015).

A interoperabilidade semântica é mais complexa. Dois dispositivos podem enviar mensagens tecnicamente válidas, mas com significados diferentes. Por exemplo, “level” pode representar nível de água, nível de bateria, nível de estoque ou nível de iluminação. Sem metadados, ontologias ou modelos de contexto, a automação pode interpretar dados de forma incorreta (PERERA et al., 2014; W3C, 2023).

A interoperabilidade organizacional envolve acordos de governança, responsabilidade, segurança, atualização, propriedade dos dados, qualidade da informação e níveis de serviço. Em cidades inteligentes, por exemplo, dados podem vir de secretarias municipais, concessionárias, empresas privadas, sensores comunitários e plataformas públicas. Integrar esses atores exige governança, não apenas tecnologia (ZANELLA et al., 2014; KITCHIN, 2014).

A ausência de interoperabilidade produz efeitos negativos. Integrações ponto a ponto tornam-se caras e frágeis. A troca de fornecedor torna-se difícil. Dados ficam presos em silos. A manutenção torna-se complexa. A escalabilidade diminui. A segurança é comprometida por soluções improvisadas. A inovação desacelera porque cada nova aplicação precisa reconstruir integrações já existentes (ATZORI; IERA; MORABITO, 2010; NOURA; ATIQUZZAMAN; GAEDKE, 2019).

A interoperabilidade, portanto, deve ser considerada requisito arquitetural desde o início do projeto. Sistemas IoT projetados sem interoperabilidade tendem a gerar ecossistemas fechados, dependentes de fornecedores e difíceis de evoluir. Em redes inteligentes de grande escala, essa limitação compromete a

sustentabilidade técnica e econômica da operação (GUBBI et al., 2013; W3C, 2023).

5. PROTOCOLOS DE COMUNICAÇÃO EM REDES IOT

Os protocolos de comunicação são componentes centrais da IoT, pois definem como mensagens são trocadas entre dispositivos, gateways, plataformas e aplicações. A escolha do protocolo influencia consumo energético, latência, confiabilidade, escalabilidade, segurança e interoperabilidade. Em ecossistemas heterogêneos, diferentes protocolos coexistem conforme requisitos do domínio (AL-FUQAHA et al., 2015; BORGIA, 2014).

O MQTT é um protocolo leve baseado no modelo publish/subscribe, amplamente utilizado em IoT por sua simplicidade, baixa sobrecarga e adequação a redes com largura de banda limitada. Dispositivos publicam mensagens em tópicos, enquanto clientes interessados assinam esses tópicos por meio de um broker. Esse modelo desacopla produtores e consumidores, favorecendo escalabilidade e flexibilidade (BANKS et al., 2019; MQTT.ORG, 2024).

O CoAP, padronizado pelo IETF no RFC 7252, foi projetado para dispositivos restritos e redes limitadas. Inspirado no modelo REST, utiliza UDP e permite operações similares a HTTP, como GET, POST, PUT e DELETE. Sua adequação a dispositivos de baixa capacidade torna-o relevante para sensores e aplicações embarcadas, especialmente quando combinado com 6LoWPAN e redes de baixa potência (SHELBY; HARTKE; BORMANN, 2014; KOVATSCH; MAYER; OSTERMAIER, 2012).

O HTTP continua presente em muitas aplicações IoT, especialmente na integração com APIs web e plataformas em nuvem. Embora seja

amplamente suportado, pode ser pesado para dispositivos restritos. Em muitos casos, HTTP é utilizado entre gateways e nuvem, enquanto protocolos mais leves operam entre sensores e gateways (FIELDING, 2000; AL-FUQAHA et al., 2015).

O OPC UA é amplamente utilizado em ambientes industriais por oferecer interoperabilidade, modelo de informação estruturado, segurança, descoberta de serviços e independência de plataforma. Sua relevância cresce em arquiteturas de Indústria 4.0, nas quais máquinas, sensores, controladores e sistemas corporativos precisam trocar dados de forma confiável e semântica (OPC FOUNDATION, 2023; HOPPE, 2014).

O DDS, ou Data Distribution Service, é utilizado em sistemas distribuídos de tempo real, como robótica, defesa, veículos autônomos e aplicações industriais. Seu modelo publish/subscribe com qualidade de serviço configurável permite comunicação eficiente em aplicações críticas. Embora menos popular em IoT doméstica, possui relevância em sistemas de missão crítica (PARDO-CASTELLÓTE, 2003; OBJECT MANAGEMENT GROUP, 2015).

O AMQP é outro protocolo de mensageria usado em sistemas empresariais e integração distribuída. Pode ser útil quando há necessidade de filas robustas, roteamento e confiabilidade transacional. Em IoT, tende a aparecer mais em camadas de backend e integração corporativa do que em sensores muito restritos (OASIS, 2012; AL-FUQAHA et al., 2015).

A escolha entre MQTT, CoAP, HTTP, OPC UA, DDS ou AMQP não deve ser dogmática. Cada protocolo atende a necessidades específicas. O desafio da interoperabilidade é justamente permitir que esses

protocolos coexistam por meio de gateways, brokers, adaptadores e modelos comuns de dados (NOURA; ATIQUZZAMAN; GAEDKE, 2019; W3C, 2023).

6. PADRÕES E MODELOS PARA INTEROPERABILIDADE: WOT, ONEM2M, MATTER, NGSI-LD E OPC UA

A padronização é um dos caminhos mais importantes para enfrentar a fragmentação da IoT. Entretanto, a multiplicidade de domínios faz com que diferentes padrões sejam necessários para diferentes contextos. O desafio não é escolher um único padrão universal, mas criar arquiteturas capazes de integrar padrões complementares (W3C, 2023; ONEM2M, 2024).

O W3C Web of Things propõe uma camada de abstração baseada em descrições padronizadas das “coisas”, permitindo que dispositivos e serviços IoT sejam descritos de forma interoperável. A Thing Description permite especificar propriedades, ações, eventos, protocolos e metadados, funcionando como interface semântica entre dispositivos e aplicações. A proposta do W3C busca complementar padrões existentes, e não substituí-los (W3C, 2023).

O oneM2M oferece arquitetura horizontal para comunicação máquina-a-máquina e IoT, com foco em interoperabilidade, reutilização de serviços comuns e integração entre domínios. Sua proposta inclui entidades comuns de serviço, registro, descoberta, gerenciamento de dados, segurança, assinatura, notificação e interfuncionamento com outras tecnologias. Essa abordagem é relevante para ambientes em larga escala e aplicações multissetoriais (ONEM2M, 2024; KOVACS et al., 2018).

O Matter surgiu como padrão de interoperabilidade para casas inteligentes, baseado em IP e apoiado por grandes empresas do setor. Seu objetivo é reduzir fragmentação entre ecossistemas residenciais, permitindo que dispositivos compatíveis funcionem em múltiplas plataformas. Embora seu foco principal seja smart home, o Matter ilustra a importância de padronizar descoberta, pareamento, segurança e controle em ambientes multi-fornecedor (CONNECTIVITY STANDARDS ALLIANCE, 2025; MADADI-BAROUGH et al., 2024).

O NGSI-LD, padronizado no âmbito da ETSI, oferece modelo de informação e API para gerenciamento de informações de contexto. Seu uso é relevante em cidades inteligentes, gêmeos digitais e aplicações que precisam publicar, consultar e assinar mudanças em entidades contextuais. Ao estruturar dados com relações e propriedades, o NGSI-LD favorece interoperabilidade semântica entre domínios urbanos, industriais e territoriais (ETSI, 2020; FIWARE FOUNDATION, 2023).

O OPC UA, por sua vez, é referência em interoperabilidade industrial. Sua força está na capacidade de representar não apenas valores, mas modelos de informação estruturados, hierarquias, eventos e métodos. Em ambientes industriais, essa dimensão semântica é fundamental para integrar chão de fábrica, supervisão, manutenção, sistemas corporativos e análise de dados (OPC FOUNDATION, 2023; HOPPE, 2014).

A coexistência desses padrões mostra que a interoperabilidade em IoT é plural. Residências inteligentes, cidades, indústrias, hospitais, redes elétricas e agricultura de precisão possuem requisitos diferentes. A arquitetura intermediária precisa reconhecer essa

diversidade e atuar como camada de mediação, não como imposição de uniformidade absoluta (NOURA; ATIQUZZAMAN; GAEDKE, 2019; W3C, 2023).

7. SEGURANÇA, PRIVACIDADE E CONFIANÇA EM ECOSSISTEMAS IOT

A segurança é um dos maiores desafios da IoT heterogênea. Dispositivos conectados ampliam a superfície de ataque porque combinam software, hardware, comunicação sem fio, exposição física e integração com sistemas críticos. Uma falha em um sensor, câmera, fechadura, medidor, gateway ou controlador pode comprometer privacidade, disponibilidade, integridade de dados e segurança operacional (ROMAN; ZHOU; LOPEZ, 2013; SICARI et al., 2015).

Os desafios de segurança começam no ciclo de vida do dispositivo. Muitos dispositivos IoT são implantados com senhas padrão, firmware desatualizado, ausência de atualização segura, interfaces inseguras, criptografia fraca e pouca capacidade de monitoramento. O NISTIR 8259A destaca capacidades-base de cibersegurança para dispositivos IoT, incluindo identificação do dispositivo, configuração, proteção de dados, acesso lógico, atualização de software, conscientização de estado de cibersegurança e documentação (NIST, 2020).

A autenticação é requisito fundamental. Dispositivos precisam provar sua identidade antes de ingressar na rede. Sem autenticação forte, dispositivos falsificados ou comprometidos podem enviar dados incorretos, capturar informações ou acionar comandos indevidos. Em larga escala, a gestão de identidades de dispositivos

torna-se tão importante quanto a gestão de identidades humanas (MIETTINEN; VAN OORSCHOT; SADEGHI, 2018; NIST, 2020).

A autorização define quais ações cada dispositivo ou aplicação pode realizar. Um sensor pode publicar dados, mas não deve controlar atuadores críticos. Um aplicativo residencial pode acionar lâmpadas, mas não deve acessar câmeras sem permissão. O princípio do menor privilégio é essencial para limitar danos em caso de comprometimento (SICARI et al., 2015; ROMAN; ZHOU; LOPEZ, 2013).

A criptografia protege confidencialidade e integridade das comunicações. Entretanto, dispositivos restritos podem ter limitações computacionais para algoritmos pesados. Protocolos como DTLS, TLS, OSCORE e mecanismos de segurança específicos devem ser escolhidos conforme capacidade do dispositivo e criticidade da aplicação (SHELBY; HARTKE; BORMANN, 2014; SICARI et al., 2015).

A privacidade é igualmente crítica. Dispositivos IoT coletam dados sobre ambiente, comportamento, localização, saúde, consumo, presença e hábitos cotidianos. Em residências, cidades e ambientes de trabalho, esses dados podem revelar padrões sensíveis. A interoperabilidade não deve significar compartilhamento irrestrito; deve haver governança de finalidade, consentimento, minimização e proteção (KITCHIN, 2014; SICARI et al., 2015).

A segurança também deve contemplar atualização e descomissionamento. Dispositivos sem suporte tornam-se passivos cibernéticos. A arquitetura IoT deve prever atualização segura, revogação de credenciais, substituição de chaves e remoção segura

de dispositivos ao final da vida útil (NIST, 2020; MIETTINEN; VAN OORSCHOT; SADEGHI, 2018).

Portanto, a interoperabilidade segura exige security by design. Não basta conectar dispositivos; é necessário conectar com identidade, autorização, criptografia, monitoramento, atualização e governança (ROMAN; ZHOU; LOPEZ, 2013; NIST, 2020).

8. EDGE COMPUTING, GATEWAYS E MEDIAÇÃO DISTRIBUÍDA

A computação em borda tornou-se componente estratégico para ecossistemas IoT de grande escala. Em vez de enviar todos os dados diretamente para a nuvem, parte do processamento pode ocorrer próximo aos dispositivos, em gateways, micro data centers, controladores locais ou nós de borda. Essa abordagem reduz latência, economiza largura de banda, melhora resiliência e permite funcionamento parcial mesmo quando a conexão com a nuvem falha (SHI et al., 2016; SATYANARAYANAN, 2017).

Os gateways IoT cumprem função central em ambientes heterogêneos. Eles podem traduzir protocolos, agregar dados, aplicar filtros, executar regras locais, autenticar dispositivos, comprimir mensagens, detectar anomalias, armazenar dados temporariamente e sincronizar com plataformas centrais. Em redes com dispositivos restritos, o gateway atua como ponte entre o mundo físico e a infraestrutura digital de maior capacidade (BUYYA; DASTJERDI, 2016; SHI et al., 2016).

A mediação distribuída é importante porque nem todas as decisões devem depender da nuvem. Em uma fábrica, uma resposta de segurança pode precisar ocorrer em milissegundos. Em uma cidade, um sensor de alagamento pode acionar alerta local antes da análise

central. Em uma residência, dispositivos devem continuar funcionando mesmo com instabilidade de internet. A borda amplia autonomia operacional (SATYANARAYANAN, 2017; SHI et al., 2016).

A borda também contribui para privacidade. Dados sensíveis podem ser processados localmente, enviando à nuvem apenas eventos agregados ou anonimizados. Isso é relevante em saúde, residências inteligentes, vigilância urbana e ambientes industriais. Entretanto, a borda também cria novos desafios de segurança, pois gateways distribuídos podem ser fisicamente expostos e mais difíceis de manter (SICARI et al., 2015; NIST, 2020).

Em termos de interoperabilidade, gateways podem incorporar adaptadores de protocolo. Um mesmo gateway pode receber dados por Zigbee, BLE, Modbus, LoRaWAN ou OPC UA e publicar eventos normalizados por MQTT ou NGSI-LD. Essa função reduz acoplamento entre dispositivos e aplicações, favorecendo substituição de componentes sem reescrever todo o sistema (NOURA; ATIQUEZZAMAN; GAEDKE, 2019; OPC FOUNDATION, 2023).

A orquestração de borda torna-se necessária em larga escala. Atualizar regras, modelos, certificados, adaptadores e políticas em milhares de gateways exige gestão centralizada e segura. Tecnologias de contêineres, OTA updates, observabilidade distribuída e gerenciamento de configuração são essenciais (SHI et al., 2016; SATYANARAYANAN, 2017).

Portanto, a interoperabilidade em IoT não deve depender apenas de plataformas centrais. A borda é camada fundamental para tradução, filtragem, segurança, autonomia e resiliência em redes heterogêneas (BUYA; DASTJERDI, 2016; SHI et al., 2016).

9. ARQUITETURAS ORIENTADAS A EVENTOS E MODELOS PUBLISH/SUBSCRIBE

A arquitetura orientada a eventos é adequada para IoT porque dispositivos frequentemente produzem fluxos contínuos de dados, mudanças de estado, alertas e medições. Em vez de aplicações consultarem constantemente os dispositivos, os eventos são publicados quando algo ocorre, reduzindo acoplamento e melhorando escalabilidade (EUGSTER et al., 2003; BANKS et al., 2019).

O modelo publish/subscribe é uma das bases dessa arquitetura. Produtores publicam mensagens em tópicos ou canais, consumidores assinam os tópicos de interesse e um broker coordena a distribuição. Essa separação permite que novos consumidores sejam adicionados sem modificar os dispositivos produtores, favorecendo evolução do sistema (EUGSTER et al., 2003; MQTT.ORG, 2024).

Em IoT, esse modelo é particularmente útil porque sensores podem publicar dados de forma simples, enquanto múltiplas aplicações podem consumir os mesmos eventos para monitoramento, controle, análise histórica, aprendizado de máquina ou alertas. Um sensor de qualidade do ar, por exemplo, pode alimentar simultaneamente painel urbano, sistema de saúde, modelo preditivo e API pública (ZANELLA et al., 2014; PERERA et al., 2014).

A arquitetura orientada a eventos também melhora resiliência. Se uma aplicação consumidora falha, os dispositivos podem continuar publicando. Se um novo serviço é criado, ele pode assinar tópicos existentes. Se a rede é instável, mecanismos de qualidade de serviço,

retenção e persistência podem reduzir perda de dados (BANKS et al., 2019; EUGSTER et al., 2003).

Entretanto, o modelo publish/subscribe exige governança de tópicos, metadados e segurança. Sem padronização, tópicos tornam-se caóticos, com nomes inconsistentes e difícil rastreabilidade. Sem autorização, consumidores indevidos podem acessar dados sensíveis. Sem observabilidade, falhas de entrega podem passar despercebidas (SICARI et al., 2015; BANKS et al., 2019).

Em redes inteligentes de grande escala, recomenda-se combinar broker de mensagens com catálogo de dispositivos, schema registry, políticas de acesso, monitoramento e mediação semântica. Essa combinação permite que eventos sejam não apenas transportados, mas compreendidos, validados e governados (NOURA; ATIQUZZAMAN; GAEDKE, 2019; W3C, 2023).

Assim, arquiteturas orientadas a eventos são essenciais para IoT, mas precisam ser acompanhadas de padronização, segurança e gestão semântica para evitar fragmentação (EUGSTER et al., 2003; BANKS et al., 2019).

10. INTEROPERABILIDADE SEMÂNTICA, ONTOLOGIAS E GERENCIAMENTO DE CONTEXTO

A interoperabilidade semântica é a capacidade de diferentes sistemas compreenderem o significado dos dados trocados. Em IoT, esse nível é decisivo porque dados de sensores só são úteis quando associados a contexto: o que foi medido, onde, quando, por qual dispositivo, em qual unidade, sob qual condição, com qual precisão e para qual finalidade (PERERA et al., 2014; W3C, 2023).

Ontologias e modelos semânticos ajudam a representar entidades, propriedades, relações e significados. Em cidades inteligentes, por exemplo, uma entidade “poste de iluminação” pode ter propriedades como localização, estado da lâmpada, consumo energético e sensor de presença. Em agricultura, uma entidade “talhão” pode estar relacionada a umidade do solo, temperatura, cultura plantada e sistema de irrigação (KOVACS et al., 2018; ETSI, 2020).

O W3C Web of Things contribui ao permitir descrições padronizadas de coisas, propriedades, ações e eventos. Essa descrição facilita descoberta automática, integração e uso de dispositivos por diferentes aplicações. A camada semântica reduz a dependência de conhecimento manual sobre cada dispositivo (W3C, 2023).

O NGSI-LD também favorece gerenciamento de contexto, permitindo representar entidades, propriedades e relações em um modelo baseado em linked data. Essa abordagem é útil para cidades inteligentes, gêmeos digitais e aplicações interdomínio, nas quais dados de transporte, clima, energia, saneamento e segurança precisam ser integrados (ETSI, 2020; FIWARE FOUNDATION, 2023).

A interoperabilidade semântica reduz erros. Um sistema que interpreta corretamente unidade, localização e tipo de sensor evita decisões equivocadas. Um dado de “nível” sem semântica pode ser ambíguo; um dado descrito como “nível de água em canal urbano, medido em centímetros, na coordenada X, com sensor Y” torna-se operacionalmente confiável (PERERA et al., 2014; W3C, 2023).

Entretanto, a semântica adiciona complexidade. Ontologias podem ser difíceis de construir, manter e alinhar entre domínios. Por isso,

recomenda-se abordagem incremental: iniciar com modelos mínimos, vocabulários controlados, metadados essenciais e evolução progressiva. A interoperabilidade perfeita não deve ser pré-condição para começar, mas deve orientar a arquitetura (NOURA; ATIQUEZZAMAN; GAEDKE, 2019; KOVACS et al., 2018).

O gerenciamento de contexto é especialmente importante em sistemas adaptativos. Um mesmo dado pode exigir respostas diferentes conforme horário, localização, criticidade, histórico e estado do sistema. Uma temperatura elevada pode ser normal em uma máquina industrial, mas crítica em um refrigerador de vacinas. O contexto transforma dado em decisão (PERERA et al., 2014; ZANELLA et al., 2014).

Portanto, a interoperabilidade semântica é a ponte entre conectividade e inteligência. Sem semântica, a IoT produz dados; com semântica, produz informação contextualizável e acionável (W3C, 2023; ETSI, 2020).

11. ARQUITETURA AIM-IOT: PROPOSTA DE MEDIAÇÃO PARA IOT HETEROGÊNEA

Este artigo propõe a **AIM-IoT — Arquitetura Intermediária de Mediação para IoT Heterogênea**, concebida para integrar dispositivos, protocolos, dados e aplicações em ecossistemas distribuídos de grande escala. A arquitetura não substitui padrões existentes; sua função é criar uma camada de mediação capaz de reduzir acoplamento, padronizar troca de informações, aplicar segurança e promover interoperabilidade evolutiva (NOURA; ATIQUEZZAMAN; GAEDKE, 2019; W3C, 2023).

A AIM-IoT possui oito camadas principais: camada de dispositivos, camada de conectividade, camada de gateway e borda, camada de adaptação de protocolos, camada de normalização de dados, camada semântica e contexto, camada de segurança e identidade, e camada de aplicações e governança. Essas camadas operam de forma integrada, permitindo que dispositivos heterogêneos participem de um ecossistema comum (AL-FUQAHA et al., 2015; SHI et al., 2016).

A camada de dispositivos inclui sensores, atuadores, máquinas, equipamentos, câmeras, medidores, wearables, controladores e sistemas embarcados. Essa camada reconhece diversidade de capacidade computacional, energia, protocolos e ciclos de vida. O modelo não exige uniformidade dos dispositivos, mas sua descrição e integração controlada (ATZORI; IERA; MORABITO, 2010; GUBBI et al., 2013).

A camada de conectividade inclui tecnologias como Wi-Fi, Ethernet, BLE, Zigbee, Thread, LoRaWAN, NB-IoT, 5G e redes industriais. Sua função é garantir transporte físico e lógico conforme requisitos de alcance, energia, largura de banda e latência. A arquitetura admite múltiplas conectividades, desde que mediadas por gateways ou adaptadores (AL-FUQAHA et al., 2015; SHELBY; BORMANN, 2009).

A camada de gateway e borda executa funções locais de agregação, filtragem, pré-processamento, autenticação, armazenamento temporário, adaptação e resposta rápida. Essa camada reduz dependência da nuvem e melhora resiliência em ambientes com conectividade instável (SHI et al., 2016; SATYANARAYANAN, 2017).

A camada de adaptação de protocolos converte mensagens entre MQTT, CoAP, HTTP, OPC UA, Modbus, AMQP ou outros protocolos. Essa conversão deve preservar metadados, qualidade de serviço e segurança sempre que possível. Adaptadores evitam integrações ponto a ponto e permitem evolução tecnológica sem reconstrução completa (BANKS et al., 2019; SHELBY; HARTKE; BORMANN, 2014).

A camada de normalização de dados transforma diferentes formatos em representações padronizadas. Pode usar JSON, CBOR, SenML, schemas versionados ou modelos definidos pela organização. O objetivo é garantir que dados de dispositivos diferentes possam ser processados por aplicações comuns (PERERA et al., 2014; AL-FUQAHA et al., 2015).

A camada semântica e contexto associa significado aos dados. Utiliza descrições de coisas, ontologias, NGS-LD, Thing Descriptions, metadados de localização, unidade, precisão, estado e relacionamento entre entidades. Essa camada é responsável por transformar mensagens em informação compreensível e interoperável (W3C, 2023; ETSI, 2020).

A camada de segurança e identidade gerencia autenticação, autorização, certificados, chaves, atualização segura, políticas de acesso, logs e detecção de anomalias. Sua função é impedir que a interoperabilidade se torne vulnerabilidade. Cada dispositivo deve ser identificado, autorizado e monitorado (NIST, 2020; SICARI et al., 2015).

A camada de aplicações e governança disponibiliza APIs, dashboards, gêmeos digitais, sistemas analíticos, aplicações móveis, automação, relatórios e integração com sistemas corporativos.

Também define políticas de propriedade dos dados, retenção, privacidade, qualidade, auditoria e níveis de serviço (KITCHIN, 2014; W3C, 2023).

A AIM-IoT opera com o princípio de interoperabilidade progressiva. Em vez de exigir que todos os dispositivos sejam substituídos, a arquitetura permite integrar gradualmente sistemas legados, novos sensores e plataformas distintas por meio de adaptadores, gateways e modelos semânticos. Essa característica é essencial para cidades, indústrias e organizações que não podem reconstruir toda a infraestrutura de uma só vez (OPC FOUNDATION, 2023; NOURA; ATIQUZZAMAN; GAEDKE, 2019).

12. APLICABILIDADE EM REDES INDUSTRIAIS, URBANAS E RESIDENCIAIS INTELIGENTES

A aplicabilidade da AIM-IoT pode ser observada em diferentes domínios. Na indústria, a heterogeneidade é marcada pela coexistência de máquinas antigas, controladores industriais, sensores modernos, sistemas SCADA, plataformas MES, ERP e serviços de analytics. A interoperabilidade entre esses sistemas é requisito para manutenção preditiva, eficiência energética, rastreabilidade e Indústria 4.0 (OPC FOUNDATION, 2023; LEE; BAGHERI; KAO, 2015).

Em ambientes industriais, OPC UA pode atuar como padrão de integração semântica entre equipamentos, enquanto MQTT pode transportar eventos para plataformas analíticas. Gateways industriais podem converter dados de Modbus, Profibus ou protocolos proprietários para formatos interoperáveis. A AIM-IoT permite

organizar essas conversões sem perder contexto operacional (OPC FOUNDATION, 2023; BANKS et al., 2019).

Nas cidades inteligentes, a interoperabilidade é ainda mais complexa. Sensores de tráfego, iluminação pública, drenagem, qualidade do ar, segurança, energia, resíduos, transporte e defesa civil frequentemente pertencem a órgãos e fornecedores distintos. Uma arquitetura intermediária permite integrar dados em modelos de contexto, APIs urbanas e gêmeos digitais (ZANELLA et al., 2014; ETSI, 2020).

Em aplicações urbanas, NGSI-LD pode representar entidades como semáforos, ônibus, sensores ambientais, pontos de alagamento, luminárias e equipamentos públicos. MQTT pode transportar eventos de sensores em tempo real, enquanto APIs permitem consulta e integração com dashboards. Essa combinação favorece gestão urbana orientada por dados (FIWARE FOUNDATION, 2023; ZANELLA et al., 2014).

No ambiente residencial inteligente, o desafio é integrar dispositivos de fabricantes e plataformas diferentes. O Matter busca reduzir fragmentação em smart homes, mas ainda coexistem Wi-Fi, Thread, Zigbee, Bluetooth, plataformas proprietárias e assistentes virtuais. Gateways e controladores interoperáveis continuam relevantes para garantir experiência integrada (CONNECTIVITY STANDARDS ALLIANCE, 2025; MADADI-BAROUGH et al., 2024).

Na agricultura inteligente, sensores de umidade, estações climáticas, bombas, drones, sistemas de irrigação, armadilhas digitais e plataformas de gestão agrícola precisam trocar dados em áreas com conectividade limitada. A borda, protocolos leves e redes de longo

alcance são fundamentais. A AIM-IoT pode adaptar conectividade LoRaWAN, armazenamento local e sincronização com nuvem quando disponível (AYAZ et al., 2019; SHI et al., 2016).

Na saúde conectada, interoperabilidade e segurança são ainda mais sensíveis. Dispositivos vestíveis, sensores domiciliares, sistemas hospitalares e plataformas de telemonitoramento lidam com dados pessoais e clínicos. A arquitetura deve priorizar privacidade, consentimento, criptografia e conformidade regulatória (SICARI et al., 2015; NIST, 2020).

Esses exemplos demonstram que a interoperabilidade IoT não é problema restrito à engenharia de redes. Ela afeta produtividade industrial, eficiência urbana, conforto residencial, segurança de pacientes, sustentabilidade agrícola e qualidade dos serviços digitais (GUBBI et al., 2013; AL-FUQAHA et al., 2015).

13. OBSERVABILIDADE, CONFIABILIDADE E MANUTENÇÃO DE REDES IOT EM GRANDE ESCALA

Redes IoT de grande escala exigem observabilidade contínua. Não basta saber que dispositivos estão conectados; é necessário monitorar qualidade da comunicação, latência, perda de pacotes, consumo energético, estado de bateria, versão de firmware, falhas de autenticação, anomalias de dados e disponibilidade dos gateways. Sem observabilidade, falhas silenciosas podem comprometer decisões automatizadas (BARROSO; HÖLZLE; RANGANATHAN, 2018; NIST, 2020).

A confiabilidade em IoT é desafiadora porque dispositivos podem falhar por bateria descarregada, interferência, dano físico, firmware corrompido, perda de conectividade, ataques, obsolescência ou

condições ambientais adversas. Sistemas robustos precisam tolerar falhas parciais e operar com dados incompletos quando necessário (TANENBAUM; VAN STEEN, 2017; AL-FUQAHA et al., 2015).

A manutenção de dispositivos deve ser planejada desde o projeto. Atualizações OTA, inventário de dispositivos, gestão de certificados, monitoramento de versões e substituição programada são elementos indispensáveis. Dispositivos abandonados sem atualização representam risco técnico e cibernético (NIST, 2020; MIETTINEN; VAN OORSCHOT; SADEGHI, 2018).

A qualidade dos dados também precisa ser monitorada. Sensores podem descalibrar, enviar leituras fora do padrão, repetir valores, produzir ruído ou parar de transmitir. A arquitetura deve incluir validação, detecção de outliers, comparação entre sensores próximos e regras de confiabilidade. Dados ruins podem ser mais perigosos que ausência de dados, pois induzem decisões equivocadas (PERERA et al., 2014; KITCHIN, 2014).

A observabilidade deve alcançar também a camada semântica. Mudanças em schemas, unidades, nomes de propriedades ou modelos de contexto podem quebrar integrações. Por isso, versionamento de modelos, documentação e testes de compatibilidade são essenciais (W3C, 2023; ETSI, 2020).

Em grande escala, a automação é necessária. Não é viável gerenciar manualmente milhares de dispositivos. Ferramentas de device management, provisionamento automático, políticas de configuração, rotação de chaves, monitoramento centralizado e dashboards operacionais tornam-se essenciais (NIST, 2020; ONEM2M, 2024).

Portanto, a interoperabilidade precisa ser acompanhada de observabilidade e manutenção contínua. Conectar é apenas o início; manter conectado, seguro e confiável é o verdadeiro desafio operacional (SICARI et al., 2015; TANENBAUM; VAN STEEN, 2017).

14. RESULTADOS DA ANÁLISE

A análise da literatura permite identificar oito resultados principais.

O primeiro resultado é que a heterogeneidade é característica estrutural da IoT, e não anomalia temporária. Dispositivos, protocolos, dados, plataformas e domínios continuarão diversos, exigindo arquiteturas de mediação e não apenas padronização rígida (ATZORI; IERA; MORABITO, 2010; NOURA; ATIQUZZAMAN; GAEDKE, 2019).

O segundo resultado é que a interoperabilidade deve ser abordada em múltiplos níveis: técnico, sintático, semântico e organizacional. A integração física de redes não garante compreensão dos dados nem coordenação operacional (W3C, 2023; PERERA et al., 2014).

O terceiro resultado é que protocolos como MQTT, CoAP, HTTP, OPC UA, AMQP e DDS possuem papéis complementares. A escolha depende de restrição energética, latência, confiabilidade, domínio de aplicação e requisitos de segurança (BANKS et al., 2019; SHELBY; HARTKE; BORMANN, 2014).

O quarto resultado é que padrões como W3C Web of Things, oneM2M, NGSI-LD, OPC UA e Matter contribuem para reduzir fragmentação, mas não eliminam a necessidade de arquiteturas intermediárias capazes de integrar sistemas legados e novos

dispositivos (ONEM2M, 2024; W3C, 2023; CONNECTIVITY STANDARDS ALLIANCE, 2025).

O quinto resultado é que a computação em borda e os gateways são componentes estratégicos para tradução de protocolos, redução de latência, autonomia local, filtragem de dados e resiliência operacional (SHI et al., 2016; SATYANARAYANAN, 2017).

O sexto resultado é que a segurança deve ser incorporada desde o projeto, contemplando identidade de dispositivos, autenticação, autorização, criptografia, atualização segura, monitoramento e descomissionamento (NIST, 2020; SICARI et al., 2015).

O sétimo resultado é que a interoperabilidade semântica é indispensável para redes inteligentes. Sem modelos de contexto, os dados circulam, mas não necessariamente produzem inteligência confiável (PERERA et al., 2014; ETSI, 2020).

O oitavo resultado é que a AIM-IoT proposta oferece uma estrutura conceitual capaz de organizar camadas de conectividade, adaptação, normalização, semântica, segurança, observabilidade e governança em ecossistemas IoT heterogêneos (NOURA; ATIQUZZAMAN; GAEDKE, 2019; AL-FUQAHA et al., 2015).

15. DISCUSSÃO

A discussão central deste artigo é que a interoperabilidade em IoT não pode ser tratada como problema secundário ou posterior à implantação dos dispositivos. Em redes inteligentes de grande escala, a interoperabilidade é condição de existência do ecossistema. Sem ela, cada dispositivo torna-se ilha tecnológica, cada fornecedor cria dependência específica e cada integração exige esforço manual,

elevando custos, riscos e fragilidade operacional (ATZORI; IERA; MORABITO, 2010; GUBBI et al., 2013).

O primeiro ponto de discussão refere-se à fragmentação. A IoT cresceu rapidamente, mas sua expansão ocorreu por domínios, fabricantes e plataformas diferentes. Essa fragmentação é compreensível, pois aplicações industriais, residenciais, urbanas e agrícolas possuem requisitos distintos. Contudo, quando não há arquitetura de mediação, a fragmentação impede escala e inovação (BORGIA, 2014; NOURA; ATIQUZZAMAN; GAEDKE, 2019).

O segundo ponto é que padronização absoluta é improvável. A diversidade de protocolos e padrões continuará existindo porque a IoT abrange desde sensores de centavos até máquinas industriais críticas. Por isso, a solução mais realista é a interoperabilidade por camadas, com gateways, brokers, adaptadores, APIs, ontologias e modelos de contexto (W3C, 2023; ONEM2M, 2024).

O terceiro ponto envolve a semântica. Sistemas IoT não precisam apenas transmitir dados, mas compreender o que os dados significam. A ausência de semântica limita automação, inteligência artificial, gêmeos digitais e análise preditiva. A interoperabilidade semântica é o passo que transforma conectividade em inteligência operacional (PERERA et al., 2014; ETSI, 2020).

O quarto ponto refere-se à segurança. Quanto mais interoperável é um ecossistema, maior pode ser sua superfície de ataque se não houver governança. A troca padronizada de informações deve ser acompanhada por autenticação, autorização, criptografia, segmentação, monitoramento e atualização segura.

Interoperabilidade sem segurança pode ampliar vulnerabilidades (ROMAN; ZHOU; LOPEZ, 2013; NIST, 2020).

O quinto ponto é a relevância da borda. Em muitos ambientes, especialmente industriais, urbanos e agrícolas, a nuvem não pode ser o único ponto de inteligência. Gateways e edge computing permitem resposta local, redução de latência, economia de rede e maior resiliência. A borda torna-se espaço de mediação técnica e semântica (SHI et al., 2016; SATYANARAYANAN, 2017).

O sexto ponto envolve governança de dados. Em ecossistemas IoT, os dados podem pertencer a dispositivos, usuários, empresas, governos ou comunidades. A arquitetura precisa definir quem pode acessar, processar, compartilhar, reter e excluir dados. Sem governança, a interoperabilidade pode gerar conflitos jurídicos, éticos e operacionais (KITCHIN, 2014; SICARI et al., 2015).

O sétimo ponto refere-se à escalabilidade. Redes pequenas podem funcionar com integrações manuais; redes grandes não. Quando o número de dispositivos cresce, torna-se indispensável automatizar descoberta, provisionamento, atualização, monitoramento e gerenciamento de identidade. A escalabilidade exige arquitetura, não improvisado (AL-FUQAHA et al., 2015; NIST, 2020).

O oitavo ponto é a dependência de fornecedores. Ecossistemas fechados podem ser rápidos no início, mas dificultam expansão, substituição e integração futura. Padrões abertos e arquiteturas intermediárias reduzem aprisionamento tecnológico e ampliam liberdade de inovação (W3C, 2023; CONNECTIVITY STANDARDS ALLIANCE, 2025).

O nono ponto refere-se à confiabilidade. Redes IoT operam em ambientes sujeitos a falhas, interferência, perda de energia, condições climáticas, ataques e degradação física. A arquitetura deve assumir falhas como inevitáveis e projetar redundância, observabilidade e tolerância a falhas (TANENBAUM; VAN STEEN, 2017; AL-FUQAHA et al., 2015).

O décimo ponto é que a interoperabilidade deve ser vista como investimento estratégico. Embora exija planejamento inicial maior, reduz custos futuros de integração, manutenção, expansão e migração. Em cidades, indústrias e residências inteligentes, a capacidade de integrar novos dispositivos sem reconstruir toda a infraestrutura é vantagem decisiva (NOURA; ATIQUZZAMAN; GAEDKE, 2019; W3C, 2023).

Assim, a AIM-IoT proposta neste artigo representa uma resposta arquitetural ao desafio da heterogeneidade. Ao organizar camadas de conectividade, gateways, adaptação de protocolos, normalização, semântica, segurança e governança, o modelo permite que ecossistemas diferentes dialoguem sem exigir uniformidade absoluta. Essa abordagem é coerente com a realidade plural da IoT contemporânea (AL-FUQAHA et al., 2015; ONEM2M, 2024).

Conclui-se que o futuro das redes IoT inteligentes dependerá menos da proliferação isolada de dispositivos e mais da capacidade de construir ecossistemas interoperáveis, seguros e semanticamente compreensíveis. A conectividade por si só não basta; é necessário construir confiança, significado e governança (SICARI et al., 2015; W3C, 2023).

16. DIRETRIZES PARA ECOSISTEMAS IOT INTEROPERÁVEIS E ESCALÁVEIS

A partir da análise realizada, propõem-se diretrizes para implantação de ecossistemas IoT heterogêneos interoperáveis.

Primeiro, definir requisitos de interoperabilidade desde a fase de projeto, contemplando conectividade, protocolos, dados, semântica, segurança e governança (NOURA; ATIQUZZAMAN; GAEDKE, 2019).

Segundo, evitar integrações ponto a ponto sempre que possível, priorizando brokers, gateways, APIs padronizadas e camadas intermediárias de mediação (EUGSTER et al., 2003; BANKS et al., 2019).

Terceiro, selecionar protocolos conforme requisitos técnicos: MQTT para mensageria leve e publish/subscribe; CoAP para dispositivos restritos; OPC UA para ambientes industriais; NGSI-LD para contexto; HTTP para integração web; e Matter para interoperabilidade residencial quando aplicável (BANKS et al., 2019; SHELBY; HARTKE; BORMANN, 2014; OPC FOUNDATION, 2023).

Quarto, adotar modelos semânticos progressivos, começando por metadados essenciais, unidades, localização, tipo de dispositivo, precisão e significado da medição (PERERA et al., 2014; W3C, 2023).

Quinto, utilizar gateways de borda para tradução de protocolos, filtragem, pré-processamento, segurança local e autonomia operacional (SHI et al., 2016; SATYANARAYANAN, 2017).

Sexto, implementar identidade única para dispositivos, autenticação forte, autorização granular e gestão segura de credenciais (NIST,

2020; SICARI et al., 2015).

Sétimo, garantir atualização segura de firmware, rotação de chaves e descomissionamento controlado de dispositivos ao final da vida útil (NIST, 2020; MIETTINEN; VAN OORSCHOT; SADEGHI, 2018).

Oitavo, padronizar tópicos, schemas, APIs e modelos de dados, evitando crescimento desordenado da arquitetura (BANKS et al., 2019; ETSI, 2020).

Nono, adotar observabilidade ponta a ponta, monitorando dispositivos, gateways, brokers, aplicações, latência, perda de pacotes, consumo energético e qualidade dos dados (TANENBAUM; VAN STEEN, 2017; NIST, 2020).

Décimo, projetar tolerância a falhas, considerando comunicação intermitente, armazenamento local temporário, reenvio de mensagens e operação degradada (AL-FUQAHA et al., 2015; SHI et al., 2016).

Décimo primeiro, separar dados sensíveis, aplicar minimização, criptografia e políticas de privacidade conforme criticidade da aplicação (SICARI et al., 2015; KITCHIN, 2014).

Décimo segundo, evitar aprisionamento tecnológico por meio de padrões abertos, documentação e APIs portáteis (W3C, 2023; ONEM2M, 2024).

Décimo terceiro, planejar escalabilidade operacional, incluindo provisionamento automático, inventário de dispositivos, monitoramento e atualização em massa (NIST, 2020).

Décimo quarto, envolver equipes multidisciplinares, pois IoT exige conhecimento de redes, segurança, software, hardware, domínio de aplicação e governança (ATZORI; IERA; MORABITO, 2010; GUBBI et al., 2013).

Décimo quinto, compreender interoperabilidade como processo contínuo, e não como entrega única. Novos dispositivos, padrões e ameaças exigem evolução permanente (NOURA; ATIQUZZAMAN; GAEDKE, 2019; W3C, 2023).

17. CONSIDERAÇÕES FINAIS

A interoperabilidade e a conectividade são condições estruturais para a consolidação da Internet das Coisas em larga escala. À medida que sensores, atuadores, máquinas, plataformas, dispositivos residenciais, sistemas urbanos e aplicações industriais se multiplicam, cresce também a complexidade de integrar tecnologias heterogêneas de forma segura, confiável e escalável (ATZORI; IERA; MORABITO, 2010; AL-FUQAHA et al., 2015).

O estudo demonstrou que a heterogeneidade da IoT ocorre em múltiplos níveis: dispositivos, conectividade, protocolos, formatos, semântica, segurança, governança e aplicações. Essa diversidade não será eliminada por um único padrão universal. Por isso, ecossistemas inteligentes precisam de arquiteturas intermediárias capazes de adaptar, normalizar, contextualizar e proteger a troca de informações (NOURA; ATIQUZZAMAN; GAEDKE, 2019; W3C, 2023).

Protocolos como MQTT, CoAP, HTTP, OPC UA, AMQP e DDS possuem papéis complementares. Padrões como W3C Web of Things, oneM2M, NGSI-LD, OPC UA e Matter contribuem para reduzir fragmentação em domínios específicos. Contudo, a

integração efetiva exige gateways, middleware, brokers, modelos semânticos, APIs e governança (BANKS et al., 2019; SHELBY; HARTKE; BORMANN, 2014; ONEM2M, 2024).

A arquitetura AIM-IoT proposta neste artigo oferece uma estrutura conceitual para redes IoT heterogêneas, organizada em camadas de dispositivos, conectividade, borda, adaptação de protocolos, normalização de dados, semântica, segurança, aplicações e governança. Essa abordagem permite integração progressiva de sistemas legados, novos dispositivos e plataformas distribuídas (SHI et al., 2016; W3C, 2023).

A análise também evidenciou que segurança e interoperabilidade devem caminhar juntas. Conectar dispositivos sem identidade, autenticação, autorização, criptografia, atualização segura e monitoramento amplia riscos cibernéticos. A segurança deve ser requisito arquitetural desde o projeto, especialmente em aplicações industriais, urbanas, residenciais e de saúde (ROMAN; ZHOU; LOPEZ, 2013; NIST, 2020).

Conclui-se que o futuro da IoT dependerá da capacidade de construir ecossistemas abertos, escaláveis, semanticamente interoperáveis, seguros e governados. A conectividade isolada cria redes de dispositivos; a interoperabilidade cria ecossistemas inteligentes. Para aplicações industriais, urbanas, agrícolas, ambientais, logísticas e residenciais, essa diferença será determinante para confiabilidade, inovação e sustentabilidade operacional.

REFERÊNCIAS BIBLIOGRÁFICAS

AL-FUQAHA, Ala; GUIZANI, Mohsen; MOHAMMADI, Mehdi; ALEDHARI, Mohammed; AYYASH, Moussa. Internet of Things: a survey on enabling technologies, protocols, and applications. **IEEE Communications Surveys & Tutorials**, v. 17, n. 4, p. 2347-2376, 2015.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The Internet of Things: a survey. **Computer Networks**, v. 54, n. 15, p. 2787-2805, 2010.

AYAZ, Muhammad; AMMAD-UDDIN, Mohammed; SHARIF, Zubair; MANSOUR, Ali; AGGOUNE, El-Hadi M. Internet-of-Things based smart agriculture: toward making the fields talk. **IEEE Access**, v. 7, p. 129551-129583, 2019.

BANKS, Andrew; BRIGGS, Ed; BORGHOFF, Ken; GUPTA, Rahul. **MQTT Version 5.0**. OASIS Standard. Burlington: OASIS, 2019.

BORGIA, Eleonora. The Internet of Things vision: key features, applications and open issues. **Computer Communications**, v. 54, p. 1-31, 2014.

BUYYA, Rajkumar; DASTJERDI, Amir Vahid. **Internet of Things: principles and paradigms**. Cambridge: Morgan Kaufmann, 2016.

CONNECTIVITY STANDARDS ALLIANCE. **Matter specification and developer resources**. Davis: Connectivity Standards Alliance, 2025.

CRESWELL, John W. **Research design: qualitative, quantitative, and mixed methods approaches**. 4. ed. Thousand Oaks: SAGE, 2014.

ETSI. **ETSI GS CIM 009: Context Information Management API, NGSI-LD**. Sophia Antipolis: European Telecommunications Standards Institute, 2020.

EUGSTER, Patrick Th.; FELBER, Pascal A.; GUERRAOUI, Rachid; KERMARREC, Anne-Marie. The many faces of publish/subscribe. **ACM Computing Surveys**, v. 35, n. 2, p. 114-131, 2003.

FIELDING, Roy Thomas. **Architectural styles and the design of network-based software architectures**. Doctoral dissertation. Irvine: University of California, 2000.

FIWARE FOUNDATION. **NGSI-LD for context information management**. Berlin: FIWARE Foundation, 2023.

GUBBI, Jayavardhana; BUYYA, Rajkumar; MARUSIC, Slaven; PALANISWAMI, Marimuthu. Internet of Things: a vision, architectural elements, and future directions. **Future Generation Computer Systems**, v. 29, n. 7, p. 1645-1660, 2013.

HOPPE, Stefan. OPC UA: interoperability for Industrie 4.0 and the Internet of Things. **OPC Foundation Technical Paper**, 2014.

KITCHIN, Rob. The real-time city? Big data and smart urbanism. **GeoJournal**, v. 79, p. 1-14, 2014.

KOVACS, Erno; BAUER, Martin; KIM, Jaeseok; YUN, Jaeseok; LE GALL, Franck; ZHAO, Mengxuan. Standards-based worldwide semantic interoperability for IoT. **IEEE Communications Magazine**, v. 56, n. 12, p. 40-47, 2018.

KOVATSCH, Matthias; MAYER, Simon; OSTERMAIER, Benedikt. Moving application logic from the firmware to the cloud: towards the thin server architecture for the Internet of Things. In: **Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing**. Palermo: IEEE, 2012.

LEE, Jay; BAGHERI, Behrad; KAO, Hung-An. A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. **Manufacturing Letters**, v. 3, p. 18-23, 2015.

MADADI-BAROUGH, Saeid; RUIZ-BLANCO, Pau; LIN, Jiadeng; VIDAL, Rafael; GOMEZ, Carles. Matter: IoT interoperability for smart homes. **arXiv preprint arXiv:2405.01618**, 2024.

MIETTINEN, Markus; VAN OORSCHOT, Paul C.; SADEGHI, Ahmad-Reza. Baseline functionality for security and control of commodity IoT devices and domain-controlled device lifecycle management. **arXiv preprint arXiv:1808.03071**, 2018.

MQTT.ORG. **MQTT: the standard for IoT messaging**. 2024.

NIST. **NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline**. Gaithersburg: National Institute of Standards and Technology, 2020.

NOURA, Mahda; ATIQUZZAMAN, Mohammed; GAEDKE, Martin. Interoperability in Internet of Things: taxonomies and open challenges. **Mobile Networks and Applications**, v. 24, p. 796-809, 2019.

OASIS. **Advanced Message Queuing Protocol (AMQP) Version 1.0**. OASIS Standard. Burlington: OASIS, 2012.

OBJECT MANAGEMENT GROUP. **Data Distribution Service Version 1.4**. Needham: OMG, 2015.

ONEM2M. **oneM2M technical specifications and architecture**. Sophia Antipolis: oneM2M, 2024.

OPC FOUNDATION. **OPC UA interoperability for Industrie 4.0 and IoT**. Scottsdale: OPC Foundation, 2023.

PARDO-CASTELLÓTE, Gerardo. OMG Data-Distribution Service: architectural overview. In: **23rd International Conference on Distributed Computing Systems Workshops**. Providence: IEEE, 2003.

PERERA, Charith; ZASLAVSKY, Arkady; CHRISTEN, Peter; GEORGAKOPOULOS, Dimitrios. Context aware computing for the Internet of Things: a survey. **IEEE Communications Surveys & Tutorials**, v. 16, n. 1, p. 414-454, 2014.

ROMAN, Rodrigo; ZHOU, Jianying; LOPEZ, Javier. On the features and challenges of security and privacy in distributed Internet of Things. **Computer Networks**, v. 57, n. 10, p. 2266-2279, 2013.

SANTOS, Marcela G.; AMEYED, Darine; PETRILLO, Fabio; JAAFAR, Fehmi; CHERIET, Mohamed. Internet of Things architectures: a comparative study. **arXiv preprint arXiv:2004.12936**, 2020.

SATYANARAYANAN, Mahadev. The emergence of edge computing. **Computer**, v. 50, n. 1, p. 30-39, 2017.

SHELBY, Zach; BORMANN, Carsten. **6LoWPAN: the wireless embedded Internet**. Chichester: Wiley, 2009.

SHELBY, Zach; HARTKE, Klaus; BORMANN, Carsten. **RFC 7252: The Constrained Application Protocol (CoAP)**. Fremont: Internet Engineering Task Force, 2014.

SHI, Weisong; CAO, Jie; ZHANG, Quan; LI, Youhuizi; XU, Lanyu. Edge computing: vision and challenges. **IEEE Internet of Things Journal**, v. 3, n. 5, p. 637-646, 2016.

SICARI, Sabrina; RIZZARDI, Alessandra; GRIECO, Luigi Alfredo; COEN-PORISINI, Alberto. Security, privacy and trust in Internet of Things: the road ahead. **Computer Networks**, v. 76, p. 146-164, 2015.

TANENBAUM, Andrew S.; VAN STEEN, Maarten. **Distributed systems: principles and paradigms**. 3. ed. Amsterdam: Maarten van Steen, 2017.

TORRACO, Richard J. Writing integrative literature reviews. **Human Resource Development Review**, v. 4, n. 3, p. 356-367, 2005.

W3C. **Web of Things (WoT) Architecture 1.1**. W3C Recommendation. Cambridge: World Wide Web Consortium, 2023.

WHITTEMORE, Robin; KNAFL, Kathleen. The integrative review: updated methodology. **Journal of Advanced Nursing**, v. 52, n. 5, p. 546-553, 2005.

WINTER, Tim; THUBERT, Pascal; BRANDT, Anders; et al. **RFC 6550: RPL, IPv6 Routing Protocol for Low-Power and Lossy Networks**. Fremont: Internet Engineering Task Force, 2012.

ZANELLA, Andrea; BUI, Nicola; CASTELLANI, Angelo; VANGELISTA, Lorenzo; ZORZI, Michele. Internet of Things for smart cities. **IEEE Internet of Things Journal**, v. 1, n. 1, p. 22-32, 2014.

¹ Doutor em Gestão de Projetos de Tecnologia da Informação e
Doutorando em Engenharia Elétrica pela Universidade de Brasília
(UnB). E-mail: [acesse o artigo original para visualizar o e-mail](#)